(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 January 2001 (04.01.2001)

PCT

(10) International Publication Number
WO 01/01224 A1

(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number: PCT/US00/17681

(22) International Filing Date: 28 June 2000 (28.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/141,498 28 June 1999 (28.06.1999) US

(71) Applicant: PRESIDEO, INC. [US/US]; 10305 102nd Terrace, Sebastian, FL 32958 (US).

(72) Inventors: BISHOP, Alan; Sebastian, FL (US). BLACKWELL, Scott; Melbourne, FL (US). BURKS, James; Vero Beach, FL (US). FLICKINGER, David; Merritt Island, FL (US). HOFFMAN, Thomas; Satellite Beach, FL (US). MOSS, Diane; Grant, FL (US). OTWORTH, Michael; Melbourne Beach, FL (US). PRINSTER, Vivian; Melbourne Beach, FL (US). REESE, Chad; -. SCHWEITZER, Shelia; Indian River Shores, FL (US). SCOTT, John; Sebastian, FL (US). URDANETA, Alfonso; -.

(74) Agents: GARRETT, Arthur, S. et al.; Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., 1300 I Street, N.W., Washington, DC 20005-3315 (US).

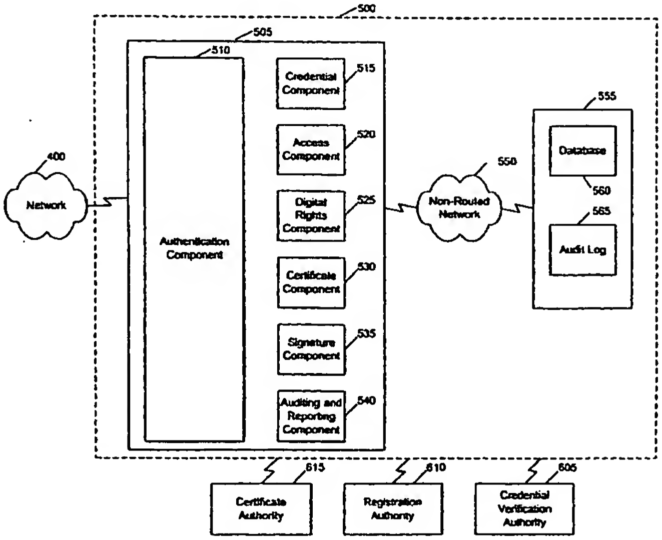
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR REGULATING ACCESS AND FOR CREATING A SECURE AND CONVENIENT COMPUTING ENVIRONMENT



(57) Abstract: An access regulation system and method are provided. The access regulation system includes a web site that includes links to resources of an organization. The system also includes an authentication component coupled to the web site for restricting access to the resources and a client terminal. The client terminal authenticates using the authentication component to gain access to the web site.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR REGULATING ACCESS AND FOR CREATING A SECURE AND CONVENIENT COMPUTING ENVIRONMENT

RELATED APPLICATION

The present application claims the benefit of U.S. provisional application no. 60/141,498, filed June 28, 1999, which is relied upon and expressly incorporated herein by reference.

BACKGROUND OF THE INVENTION

A. Field of the Invention

The present invention relates to regulating access, and more particularly, to a system and method for regulating access to resources of an organization, and for creating a secure and convenient computing environment.

B. Description of the Related Art

Most organizations want to regulate access to their resources, for example, data and computer applications. At the same time, these organizations want to create a secure and convenient computing environment for their users, such as their employees. For example, most organizations want their users to be able to access information from anywhere and anytime. To accomplish this, for example, many organizations have made some or all of their resources available to their users via an online network, such as the Internet and specifically, the World Wide Web ("Web"). The web is a distributed system that includes web servers and web clients. Web servers are software applications that support common protocols, such as Hypertext

Transport Protocol (HTTP). Moreover, these web servers make documents, such as documents in hypertext mark up language (HTML), and other resources available to users via web pages. Web clients include software applications, such as a browser, which a user uses to access a web page, for example. However, due to several drawbacks with the online networks and with the currently available authentication systems, regulating access as well as creating a secure and convenient environment has not been possible.

One drawback is that most organizations have several different applications that provide access to their resources, such as data. To access each application, a user may need a different password and may need to follow certain steps, for example, logging into the application, before the user can gain access to the application. This results in an inconvenience for both the users and the organizations. Since multiple passwords and different steps are involved, users often write their passwords and the steps that need to be followed to access that application. Written passwords and steps may be accessed by unauthorized users, who may then use the passwords and steps to gain access to the applications. Furthermore, passwords may be compromised by others. Multiple passwords and applications also create an administrative burden for the organization. For example, if a user misplaces the written passwords, the organization may need to reassign new passwords to this user, which is time consuming and inconvenient.

Another drawback is that if a user needs to go outside the physical bounds of one location of an organization, the user may no longer have access to the resources. For example, large organizations, such as hospitals, often have more than one physical location, and as a result, doctors may rotate from one location to the other. If these hospitals are connected to each other, for example, in a wide area network, the doctors may be able to access the data from any location. However, if the hospitals are not connected, the doctors may need separate accounts in each of the physical locations to gain access to the resources of each of the hospitals. Creation and maintenance of these separate accounts create inconvenience for both the users and the organizations.

Still another drawback is that although most organizations desire to verify a user's credentials both before giving a user access to their resources, and periodically, after giving the user access to their resources, these organizations currently do not have the ability to quickly check the credentials without having a detrimental effect on the organization's efficiency. As a result, many organizations do not perform such credentials validation. This may, however, result in unauthorized users having access to the resources of the organization. For example, before giving access to a user, such as a doctor, an organization, such as a hospital, may want to check the doctor's credentials, such as a doctor's good standing with appropriate governing boards. Also, once the doctor is given access to the resources, most hospitals want to check the doctor's standing periodically to ensure that the doctor is in good standing. However, this credential verification process may take several days and thus, create inconvenience for both the organization and the user. As a result, some organizations rely on a user's paper credentials rather than verifying the credentials via an independent source before giving access to the users. This paper credential verification may lead to access by unauthorized users.

Another drawback is the limited ability of a user or an organization to control the content and rights to a resource, such as a document , both within the organization and in the online network, such as the Internet. For example, most organizations want to be able to control the content of a document from one user to another user within the organization. Moreover, the organization wants to at least be certain that the document remains authentic after the document is sent to a recipient located outside of the organization. Although digital certificates may provide some control over the authenticity of the transactions or documents, these are limited. For example, an unauthorized user may be able to gain access to a user's password and may use the user's digital certificate for transactions or sending documents. Moreover, the digital certificate may be tied to a workstation instead of a user. So, if the user uses a different workstation, the user may not be able to gain access to the user's digital certificate easily. Furthermore, digital certificates may not be able to control the rights of another user over the received document. For example, a user may desire to send a document to another user in the organization, but may only want to give the other user view rights. The user may not want the recipient to have the ability of saving or printing the document. Digital certificates provide no such control.

Accordingly, there is presently a need for a system and method for regulating access to an organization's resources and for creating a secure and convenience computing environment.

SUMMARY OF THE INVENTION

An access regulation system consistent with the present invention includes a web site that includes links to resources of an organization. The system also includes an authentication component coupled to the web site for restricting access to the resources and a client terminal. The client terminal authenticates using the authentication component to gain access to the web site.

In addition to a system, the present invention provides a method for regulating access to resources of an organization. Using this method, resources are made available on a web site. Access to the web site is restricted by using an authentication component, which is coupled to the web site. A client terminal is given access to the web site after authentication to the authentication component.

The present invention also provides a computer-readable medium containing instructions for causing a computer to perform a method for regulating access to resources of an organization. In this method, resources are made available on a web site. Access to the web site is restricted by using an authentication component, which is coupled to the web site. A client terminal is given access to the web site after authentication to the authentication component.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings are incorporated in and constitute a part of this specification and, together with the description, explain the advantages and principles of the invention. In the drawings,

FIG. 1 is a diagram of an exemplary network environment in which features of the present invention may be implemented;

FIG. 2 is an exemplary block diagram illustrating components of the client terminal 100 that is shown in FIG. 1;

FIG. 3 is an exemplary block diagram illustrating components of the services system 500 that is shown in FIG. 1;

FIG. 4 is an exemplary flowchart illustrating the steps involved in setting up the services system 500 of the present invention;

FIG. 5 is an exemplary flowchart illustrating the user enrollment process in accordance with the present invention;

FIG. 6 is an exemplary flowchart illustrating the process of accessing resources in accordance with the present invention;

FIG. 7 is an exemplary flowchart illustrating the authentication process in accordance with the present invention; and

FIG. 8 is an exemplary web page illustrating the features of the present invention.

DETAILED DESCRIPTION

The following detailed description of the invention refers to the accompanying drawings. While the description includes exemplary embodiments, other embodiments are possible, and changes may be made to the embodiments described without departing from the spirit and scope of the invention. The following detailed description does not limit the invention. Instead, the scope of the invention is defined by the appended claims and their equivalents.

The present invention provides a system and method to regulate access to the resources of an organization and to create a secure and convenient computing environment for the organization's users. For example, with the use of the present invention, an organization may create a web site with links to some or all its resources, such as applications. Applications may include, both web based and non-web based applications. The web site may be customized for each user. Moreover, the web site may be hosted by the organization or a third party, and may be available anytime and from anywhere.

Furthermore, a user desiring access to the web site may be enrolled for access only after verification of the users' credentials. The verification may be done in real-time. Moreover, once the user is enrolled, the user may be required to authenticate before the user will be given access to the web site. Authentication may include, but is not limited to, the use of a biometric; a user access card, such as a smart card; and a user name and password. Biometric authentication includes the use of unique physical characteristics of a user, such as fingerprint patterns, voice, eyes, face, hand, etc., to confirm the identity of a user. Moreover, the user may use a single user name and password, for example, to gain access to all the resources.

Once authenticated to the web site, the user may have access to digital certificates, digitized signatures, and digital rights. Users may be issued digital certificates that allow them to conduct secure web transactions. These certifications may be assigned specifically to the user, not to a workstation, and thus, may allow greater user mobility and convenience. Combined with the digital certificates, the users also may be able to sign documents with a digitized signature. Furthermore, the users may be able to assign digital rights to a specific document before sending it to a recipient, who may be another user in the organization. These rights may include, for example, view only rights. As a result of these digital rights, a recipient will only be able to view the document and will not be able to, for example, print the document.

In addition, the present invention may provide the ability to audit and report. Thus, with the use of the present invention, organizations may regulate access to their resources as well as provide a secure and convenient computing environment.

The above example is intended to be illustrative of the features of the present invention as opposed to limiting it in any manner. Moreover, the system and method of the present invention are not limited to any particular organization, user, or resource. An organization may include, but is not limited to, a business, a government entity, and a non-profit organization. A user may include, but is not limited to, an employee and a customer. A resource may include, but is not limited to, data, applications, documents, and access to digitized signatures, digital certificates, and digital rights.

The above-noted features, other aspects, and principles of the present invention may be implemented in various system or network configurations to provide automated and computational tools to facilitate regulation of access and to create a secure and convenient computing environment. Such configurations and applications may be specially constructed for performing the various processes and operations of the invention or they may include a general purpose computer or computing platform selectively activated or reconfigured by program code to provide the necessary functionality. The processes disclosed herein are not inherently related to any particular computer or other apparatus, and may be implemented by a suitable combination of hardware, software, and/or firmware. For example, various general purpose machines may be used with programs written in accordance with teachings of the invention, or it may be more convenient to construct a specialized apparatus or system to perform the required methods and techniques.

The present invention also relates to computer readable media that include program instruction or program code for performing various computer-implemented operations based on the methods and processes of the invention. The media and program instructions may be those specially designed and constructed for the purposes of the invention, or they may be of the kind well-known and available to those having skill in the computer software arts. The media may take many forms including, but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical or magnetic disks. Volatile media includes, for example, dynamic memory. Transmission media includes, for example, coaxial cables, copper wire, and fiber optics. Transmission media can also take the form of acoustic or light waves, such as those generated during radio-wave and infra-red data communications. Examples of program instructions include both machine code, such as produced by compiler, and files containing a high level code that can be executed by the computer using an interpreter.

FIG. 1 is a diagram of an exemplary network environment in which features of the present invention may be implemented. The network environment includes client 100, resources 300, and services system 500, all of which are interconnected by network 400. Network 400 may be a single or a combination of any type of computer network, such as the Internet, an Intranet, an Extranet, a Local Area Network (LAN), or a Wide Area Network (WAN), for example. These as well as other network configurations are known to those skilled in the art and are also within the scope of the present invention.

Client terminal 100 of FIG. 1 may include, but is not limited to, a personal computer, a handheld computer, or any similar device known to those skilled in the art. As shown in FIG. 2, the client terminal 100 may include a browser 110, such as a world wide web browser like NETSCAPE NAVIGATOR and/or INTERNET EXPLORER; other software and data storage 120; at least one input device 130, such as a keyboard or a mouse; at least one communications device 140, such as a modem or a network interface card (NIC); at least one processor 160; memory 150; and at least one output device 170, such as a monitor; and a reading device 190, such as a biometric device or a smart card reader device, all of which may communicate with each other, for example via a communication bus 180. The biometric device may be, for example, a finger scanner that is used to scan a users' fingerprint for authentication purposes. The memory 150 may be random access memory (RAM), read only memory, or both. Other client terminals and their components are known to those skilled in the art and are also within the scope of the present invention. For example, it is known to one skilled in the art that in order for the biometric device to interface with the client 100, software drivers may be needed.

Resources 300 may include data, applications, and access to digitized signatures, digital certificates, and digital rights. Applications may be web based or non-web based applications. For example, non-web based applications may be applications, such as Microsoft Word, and other applications that are written for a particular purpose, such as a medical application written for the specific purpose of accessing a patient records. These applications may require additional steps for execution, such as logging into the application in addition to logging into a system that runs these applications.

Services system 500 shown in FIG. 1 will now be described. As shown in FIG. 3, the services system 500 includes a web server 505 and a storage server 555, which are connected to each other via a non-routed network 550, such as a non-routed LAN. The web server 505 includes authentication component 510, credential component 515, access component 520, digital rights component 525, certificate component 530, signature component 535, and auditing and reporting component 540. The storage server 555 may include a database 560 and an audit log 565. The data associated with the organization and users is stored in the database 560. Since, the non-routed network 550 may not be accessed directly from the network 400, such as the Internet, this provides a more secure computing environment because unauthorized users will not be able to gain access to the database 560 and audit log 565. Although not shown, both the web server 505 and the storage server 555 also may have an administration component for administering the various components. Moreover, in FIG. 3, the various components are shown to exist on a single web server 505 and a single storage server 555; however, it is known to one skilled in the art that these components may exist on multiple servers to assist in load balancing.

Each of the components shown in FIGs. 1-3 may use various protocols to communicate with each other. In addition, the communication between the various components may be encrypted. For example, the client 100 may communicate with the web server 505, for example, by using the Hypertext Transport Protocol (HTTP) protocol. CORBA's (Common Object Request Broker Architecture) IIOP (Internet Inter-Object Request Broker Protocol) may also be used. Moreover, the secure sockets layer (SSL) also may be used, both as a protocol and encryption. For example, 128 bit SSL encryption may be used. Other encryption algorithms, such as the Blowfish 448-Bit encryption algorithm, may be used. These and other similar protocols and encryption algorithms are known to those skilled in the art and are also within the scope of the present invention.

Some of the components shown in FIG. 3 will be briefly described now. The authentication component 510 performs all authentication related functions. The authentication component 510 is transparent to the user. The authentication component 510 may use, for example, a user name and authentication token. Authentication token may include a biometric; a user access card, such as a smart card; and/or a password. As a result of authentication tokens, such as biometric authentication, the present invention creates a secure computing environment.

Moreover, the credentialing component 515 may verify the professional credential information provided during user enrollment. The verification may take place in real-time using a credential verification authority (CVA) 605, which is shown in FIG. 3. The CVA may be a third party independent data source. If for some reason, the credentials are not verifiable using the CVA 605, a registration authority 610 may be provided for manual verifications; reviewing user profile information; and resolving discrepancies by contacting the users, the organization, and/or the CVA 605. The registration authority 610 may be an administrator, for example. The credentialing component 515 may also provide a watch list service, which monitors all enrolled users and notifies the registration authority 610 upon a change in a user's data, such as licensing status. As a result of the real-time credential verification abilities and the watch list service, the present invention assists organizations, such as hospitals, in hiring and retaining only qualified individuals.

The access component 520 may provide users with a single sign-on ability to quickly access an organization's resources, such as resources 300. Users may only need to remember, for example, one user name and one password, for access to all the resources 300. The access component 520 may be a browser based client application. Users at the client terminal 100 may access the access component 520 from a standard web browser, such as NETSCAPE NAVIGATOR or INTERNET EXPLORER. Once authenticated, the users may be presented with a customized web page, for example, that includes links to all the resources they have given access to. Example of such a web page is shown in FIG. 8. As shown in FIG. 8, the web page may include frames and one of the frames may include a list of resources that the user can access. In this example, the resources include Excel, Winword, Web Application No. 1, Medical Records, Access, and Powerpoint. With a web page, like the one shown in FIG. 8, and once the user has successfully authenticated, a user may just select the application that the user wants to execute and may not need to provide any other user names and passwords, which may be specific to a particular application, such as Medical Records. Thus, as shown in FIG. 8, access component may present a web page, which may become a start page for a user and replace the functionality provided by an operating system, for example, the desktop in Windows 95.

As a result of the access component 520 and depending on the authentication token used, the users may only need to memorize a user name and/or password. For example, if a user name and password are used, then, the user may need to remember both the user name and the password, which is the authentication token. On the other hand, if a biometric authentication token is used, the user may only need to memorize the user name and then, provide the biometric, using a reading device 190, for example. If smart cards are used, the user may not need to enter anything and may just place the card in the reading device 190, for example.

The digital rights component 525 shown in FIG. 3 will be now described. The digital component 525 may provide persistent protection of information once a user is done with the information, for example a document. This persistent protection may be provided through a set of rights that the organization assigns and applies to the content that is to be protected. These rights may be enforced at the recipient end, for example, through a browser plug-in or digital rights software installed on a recipient's machine. The content assignable rights may include, for example, access, copying, saving to disk, and printing. Even if a recipient passes the content to another recipient, the new recipient may also be required to conform to the applied access rights. Moreover, the locally stored content may be encrypted, for example, in such a manner that it can only be opened by digital rights software in conjunction with the digital rights component 525.

Specifically, the digital rights component 525 may include a builder, a clearinghouse, and content player. The builder may build the protected objects package and allow the associated rights to be set. As a result, the built package contains the protected content, such as a document, and its associated rights. Clearinghouse is a component that may either unlock or provide the mechanism to unlock the protected package. This component along with the content player may verify the integrity of the protected content and may enforces the previously applied rights. Finally, the content player runs on a user's workstation, such as client terminal 100. It may either be pre-installed or may be downloaded, as needed. The content player may ensure that the protected package remains intact and the associated rights are applied correctly. Moreover, the content player may also contact the clearinghouse to authenticate the user and to ensure that the associated rights are applied prior to allowing the user to view the content. Thus, the present invention gives the users and the organization the ability to control what happens with a document, for example, after the organization or the user sends the document to a recipient, who may be another user in the same organization.

The certificate component 530 shown in FIG. 3 will be described now. The certificate component 530 manages certificate issuance and storage. The certificate component 530 is not a certificate authority (CA). Instead, the certificate component 530 may request, renew, revoke and validate standard certificates, such as X.509v3 certificates, through a recognized certificate authority. For example, in FIG. 3, certificate authority 615 may be used as the certificate authority. All interaction with the certificate authority may be based on public-key cryptography standards (PKCS) and as a result, the present invention may be compliant with all PKCS compliant certificate authorities.

The issued certificate may be made available by the certificate component 530 as an additional verification mechanism. For example, during setup, as described with reference to FIG. 4, the organization may setup the system such that the user may be required to have a valid certificate associated with the user profile before being authenticated.

Moreover, the issued certificates may be made available for use by the enrolled user based on the organization's imposed rules. One option may be that the certificates may be downloaded and installed on the client terminal 100 through a set of predefined web pages. Another option may be that the certificate with its associated private key may be stored, for example, as an encrypted blob, for roaming access. This option may enable the certificate and the private key to be stored and distributed in such a manner that they are not decrypted until the time of use on the client terminal 100. Thus, with the present invention, the resulting digital certificate may be assigned specifically to the user rather than a workstation, such as the user's client terminal 100. This allows for greater user mobility in addition to security.

In addition to digital certificates, the present invention provides digitized signatures via the signature component 535. The signature component 535 may enable resources, such as HTML documents, to be exchanged electronically over the Web with a digital image of a user's actual signature. Additionally, the signature component 535 may allow the user to sign a document, for example, for either release or acceptance after document review. The system and method of the present invention may require a user to submit a notarized pen and paper signature, for example, via U.S. mail, which will be digitized and stored in the database 560. Moreover, the present invention provides a captured signature that may be mobile with the user and may not be tied to any particular workstation, such as client terminal 100. The electronic signature may only be released for use once the user has properly authenticated via the authentication component 510. Once signed, the document may then be electronically distributed. The electronically signed document may be then viewed from a browser, for example.

When using the signature component 535, designated documents may be electronically signed with the previously captured, legally binding, electronic signature. In one embodiment, the electronic signatures may be accessed after authentication only. The electronic signature may be used to ensure that documents have not been modified or tampered with after the electronic signature has been applied, for example, by embedding a java script. When a recipient opens the received document, the java script may obtain the user's digitized image from the database 560 and may display it to the recipient. Notification may be made to the recipient if the document is altered in any way from the time it was originally electronically signed, for example, via visual queues based on document type. As a result, the recipient of the document may easily determine if the document had been compromised since being signed. An error dialog box may be displayed. In addition, another visual queue may be that the actual sender's or user's signature may be lacking from the document.

The auditing and reporting component 540 shown in FIG. 3 will be described now. The auditing and reporting component 540 may provide an interface to all of the other components shown in FIG. 3 in order to provide report information on selected or all data fields. Access to the reports themselves may be audited and restricted to authorized users, such as administrators, who have successfully authenticated into the services system 500. For example, when a user attempts to access a report, the user may be required to enter a user name and an authentication token. After the user provides the requested information and after the information has been verified, the user may be given access to the report. In one embodiment, the auditing and reporting component 540 may provide e-mail alerts to administrators. These alerts may notify the administrator, for example, of repeated authentication failures.

The services system 500 may be hosted by the organization or a third party. However, before using the services system 500, an administrator for the organization or the third party must setup the services system 500, for example, by using the browser 110 on a client terminal 100. FIG. 4 is an exemplary flowchart illustrating the steps involved in setting up the services system 500. In a step 805, the administrator may log into the services system 500 using the browser 110, for example. Next, in a step 810, the administrator may fill in the organization's information, for example, on a web page presented by the administration component. Then, in a step 815, the administrator may select the components that the organization plans to use. For example, one organization may choose to only use the authentication component 510 and the access component 520, whereas other organizations may choose to use the authentication component 510, the access component 520, and the credentialing component 515. Next, in a step 820, the administrator may create a generic web page. This generic web page may be the first page that a user sees when the user accesses the services system 500. Then, in a step 825, the administrator may enroll users to the services system 500. The process of enrolling users will be described next by referring to FIG. 5.

With reference to FIG. 5, the process of enrolling users into the services system 500 will be explained now. The authentication component 510, the credentialing component 515, and the access component 520 assist the administrator in enrolling users to the services system 500. With the use of the browser 110 on the client 100, the administrator logs into the services system 500 if he is not already logged into the system. Once logged in, the administrator fills in a user's information, for example, on a web page presented by the access component 520, as indicated by a step 1005. The authentication component 510 may require enough user information to uniquely identify that individual within that organization. For example, such user information may include a user's full name, date of birth, social security number, passport number, and driver license information. Once such information has been entered, the access component 520 determines whether the user is already present in the system, as indicated by a step 1010. If the user is not in the system, the user is created, as indicated by step 1015.

Then, in a step 1020, the administrator is asked for a user name and an authentication token, for example, by the authentication component 510. For example, if the organization uses user name and password, the administrator may assign a user name and a password in step 1020. On the other hand, if the organization uses biometric authentication, then, the authentication component 510 may ask the administrator to capture a biometric of the user the administrator is registering. For example, a Java applet, which asks the administrator to capture a biometric, may be downloaded to the client 100 and this Java applet may talk to a secure Java servlet back on the services system 500. Once the administrator provides the biometric, for example, by scanning a user's finger with a reading device 190, such as a fingerprint scanner, the access component 520 may store the captured biometric along with the user's information in the database 560. Next, in a step 1025, the administrator assigns access rights to the user. For example, access rights may include giving the user rights to certain applications of the organization and customizing the user's starting web page. Again, the access rights that the administrator defines for the user are stored in the database 560. The access rights, the authentication token, and the user information may be stored in a user profile in the database 560, for example.

Conversely, if in step 1010, it is determined that a user already exists, the access component 520 presents a web page, for example, asking the administrator to verify user information, as indicated by a step 1027. As a result, the present invention provides the ability to an administrator to easily move users from one organization to the other without deleting the authentication token or without having to re-enter all user information. For example, in step 1027, the administrator may change any of the user information, if needed. The administrator may, for example, change the user's organization information. Thus, the present invention creates a convenient administration environment for the administrator.

Once it is determined that a user already exists and the user information has been verified, as indicated by steps 1010 and 1027, or once access rights have been assigned to the newly created user, as indicated by step 1025, the system next determines whether the credentialing component 515 has been enabled, as indicated by step 1030. As described with the description of FIG. 4, the credentialing component 515 may be enabled by the administrator during the setup process. If the credentialing component 515 is not enabled, then the administrator is done, as indicated by a step 1055. On the other hand, if the credential component 515 is enabled, the system determines whether a credential verification has been done on this user before, as indicated by a step 1035. For example, the system may query the database 560 in this step to determine if a credential verification was done in the past. If a credential verification was done, then the administrator is done, as indicated by a step 1055.

Conversely, if in the step 1035, it is determined that the credential verification was not done, the credentialing component 515 may present the user a web page, for example, asking for the user's credential information, as indicated by step 1040. For example, if the user is a doctor, credential information, may include, for example, the doctor's state license number. Once the information has been entered, the information may be submitted to a CVA 605 for verification. CVA 605 verifies the information in real-time. Once CVA 605 returns a response to the credentialing component, it is determined whether the credential verification was successful, as indicated by step 1045. If the verification was successful, the user is enrolled in the system and the user enrollment process is complete, as indicated by step 1055. On the other hand, if the credential verification was not successful, the information is sent to a registration authority 610 for manual verification. As described in the foregoing description, the CVA 615 provides manual verifications; reviews user profile information; and resolves discrepancies by contacting the users, the organization, and/or the CVA 605.

With reference to FIGs. 6 and 7, exemplary steps involved in user authentication and resource access will be described in detail now. In a step 1100, the user uses client 100 and launches browser 110, for example. Next, the user may be asked to authenticate to the system, as indicated by a step 1105. For example, the user may be provided with a web page and may be asked to enter a user name and authentication token, for example. The authentication process will be described by referring to FIG. 7. In a step 1200, the user may be prompted by the authentication component 510 for a user name and password. Then, in a step 1205, the user provides the user name and authentication token. Once the information is provided, the system uses the user name to access the authentication token that is stored in the database 560, and compares this authentication token against the token provided by the user, as indicated by a step 1210. This technique results in a one to one search and match. If there is a match, the user may be given access, as indicated by step 1215. On the other hand, if there is no match, the user may be asked to try again, as shown in FIG. 7. The number of logon attempts may be limited and the system may, for example, deny access to the user after two attempts.

An example of the authentication process will now be described for illustrative purposes. In step 1200, a Java applet may be downloaded to the user's client terminal 100, and this applet may prompt the user for a user name and authentication token. The Java applet may talk to a secure Java servlet, which is resident on the web server 505. After the user provides the user name and authentication token, these are sent back to the web server 505, as indicated by a step 1205. Then, the web server matches the received authentication token, for example, a captured finger image, against the authentication token stored in the database 560. If the captured finger image matches the stored image, the user is given access to the system. All the communication between the web server 505 and the client 110 may be 128 bit SSL encrypted. Moreover, the actual machines that do the match may be on the non-routed network 550.

Once the user is authenticated, the access component 520 may present a customized web page or a generic web page, as indicated by a step 1110. For example, during the user enrollment process, the administrator may have created a customized web page with links to all the resources that the user can access. Alternatively, the administrator may have linked a generic web page to the user's profile. For example, if the user is a doctor as opposed to a nurse, the doctor may have been given access to more resources than the nurse. Thus, the doctor may have a customized web page with more resources, whereas the nurse may have access to a generic web page. A sample web page is shown in FIG. 8.

From the web page, the user may select the resources that the user wants to access, as indicated by a step 1115. If the resource is an application, the access component 520 checks to see if a script is associated with the application, as indicated by step 1120. If a script is associated with the application, the script is retrieved and executed, as indicated by steps 1125 and 1135. As a result of the execution of the script, the application may be executed, as indicated by step 1130. For example, some applications may require a different user name and password or may require further steps before the application is launched. Scripts may be written for these type of applications. The script may include, for example, the different user name and password, and may also include commands to execute the application. As a result, the user may not need to perform any extra steps to launch such an application and may gain access to several applications without needing to remember or enter several passwords and user names. On the other hand, if the application does not have a script associated with it, the application may be executed by the user in step 1130.

The components shown in FIG. 3 of the present invention provide many advantages. For example, one advantage is that before gaining access to any of the components shown in FIG. 3 or the resources 300, a user may need to authenticate, thus creating a secure computing environment. Another advantage is that users may not need to remember multiple user names and passwords. Instead, users may only need to remember a single user name/password or a user name if a biometric is used , for example. Still another advantage is that the present invention provides for biometric authentication, which may not be compromised. In addition, even if user moves to a different location within an organization, the administrator may not need to recreate users. Instead, the administrator may be able to just change information, such as the location information, for the user. The present invention also provides the ability to ensure that a user's professional credentials are intact prior to access and the ability to verify a user's credentials periodically even after initial enrollment. Still other advantages of the present invention include the ability to provide access to a mobile digital certificate; control usage of transmitted data; assign a legally binding electronic signature to documents, and track usage activity.

While the examples given in the foregoing description related to hospitals, the present invention is not limited to the health care industry or for use within an organization. For example, an organization, such as a business that sells goods through the Internet may utilize the present invention. In that case, the customers will be the users and the customer may buy resources, such as goods, from the business using the business's web site.

It will be apparent to those skilled in the art that various modifications and variations can be made in the system and method of the present invention and in construction of this invention without departing from the scope or spirit of the invention. For example, the present invention may be modified so that an organization desiring to secure access to their web site may, initially, send a user to the services system 500, which may authenticate the users, and then, provide the customer access to the organization's web site by sending the customers back to the organization's web site.

Moreover, other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

WHAT IS CLAIMED IS:

1. An access regulation system comprising:

a web site that includes links to resources of an organization;

an authentication component coupled to the web site for restricting access to the resources; and

a client terminal, wherein the client terminal authenticates using the authentication component to gain access to the web site.

2. The access regulation system according to claim 1, further comprising an access component for regulating access to the resources and for providing single sign-on ability.

3. The access regulation system according to claim 1, wherein the authentication component supports biometric authentication.

4. The access regulation system according to claim 1, further comprising a credentialing component for verifying a user's credentials in real-time.

5. The access regulation system according to claim 1, further comprising a certificate component for providing mobile digital certificates.

6. The access regulation system according to claim 1, further comprising a digital rights component for controlling use of the resources.

7. The access regulation system according to claim 1, further comprising a signature component for assigning a legally binding electronic signature to the resources.

8. The access regulation system according to claim 1, further comprising a auditing and reporting component for tracking usage activity of the resources.

9. A method for regulating access to resources of an organization, comprising the steps of:

making the resources available on a web site;

restricting access to the resources by using an authentication component, which is coupled to the web site; and

authenticating to the authentication component using a client terminal to gain access to the web site.

10. The method according to claim 9, further comprising the step of regulating access using an access component.

11. The method according to claim 9, wherein the step of authenticating includes the use of a biometric for authentication.

12. The method according to claim 9, further comprising the step of verifying a user's credentials in real-time using the credential component.

13. The method according to claim 9, further comprising the step of providing mobile digital certificates using the certificate component.

14. The method according to claim 9, further comprising the step of controlling use of the resources using a digital rights component.

15. The method according to claim 9, further comprising the step of assigning a legally binding electronic signature to the resources using the signature component.

16. The method according to claim 9, further comprising the step of tracking usage activity of the resources using the auditing and reporting component.

17. A computer-readable medium containing instructions for causing a computer to perform a method for regulating access to resources of an organization, comprising the steps of:

making the resources available on a web site;

restricting access to the resources by using an authentication component, which is coupled to the web site; and

authenticating to the authentication component using a client terminal to gain access to the web site.

18. The computer-readable medium according to claim 17, further comprising the

step of regulating access using an access component.

19. The computer-readable medium according to claim 17, wherein the step of authenticating includes the use of a biometric for authentication.

20. The computer-readable medium according to claim 17, further comprising the step of verifying a user's credentials in real-time using the credential component.

21. The computer-readable medium according to claim 17, further comprising the step of providing mobile digital certificates using the certificate component.

22. The computer-readable medium according to claim 17, further comprising the step of controlling use of the resources using a digital rights component.

23. The computer-readable medium according to claim 17, further comprising the step of assigning a legally binding electronic signature to the resources using the signature component.

24. The computer-readable medium according to claim 17, further comprising the step of tracking usage activity of the resources using the auditing and reporting component.

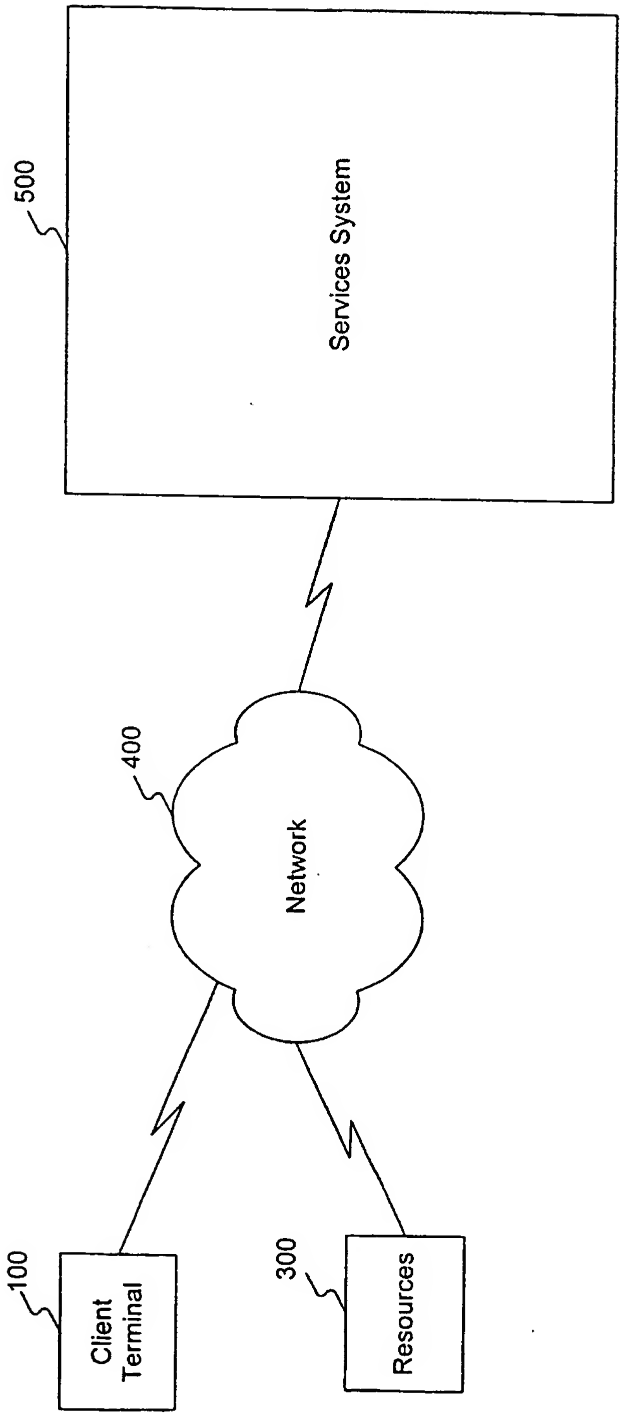

500
Services System
400
Network
100
Client Terminal
300
Resources

FIG. 1

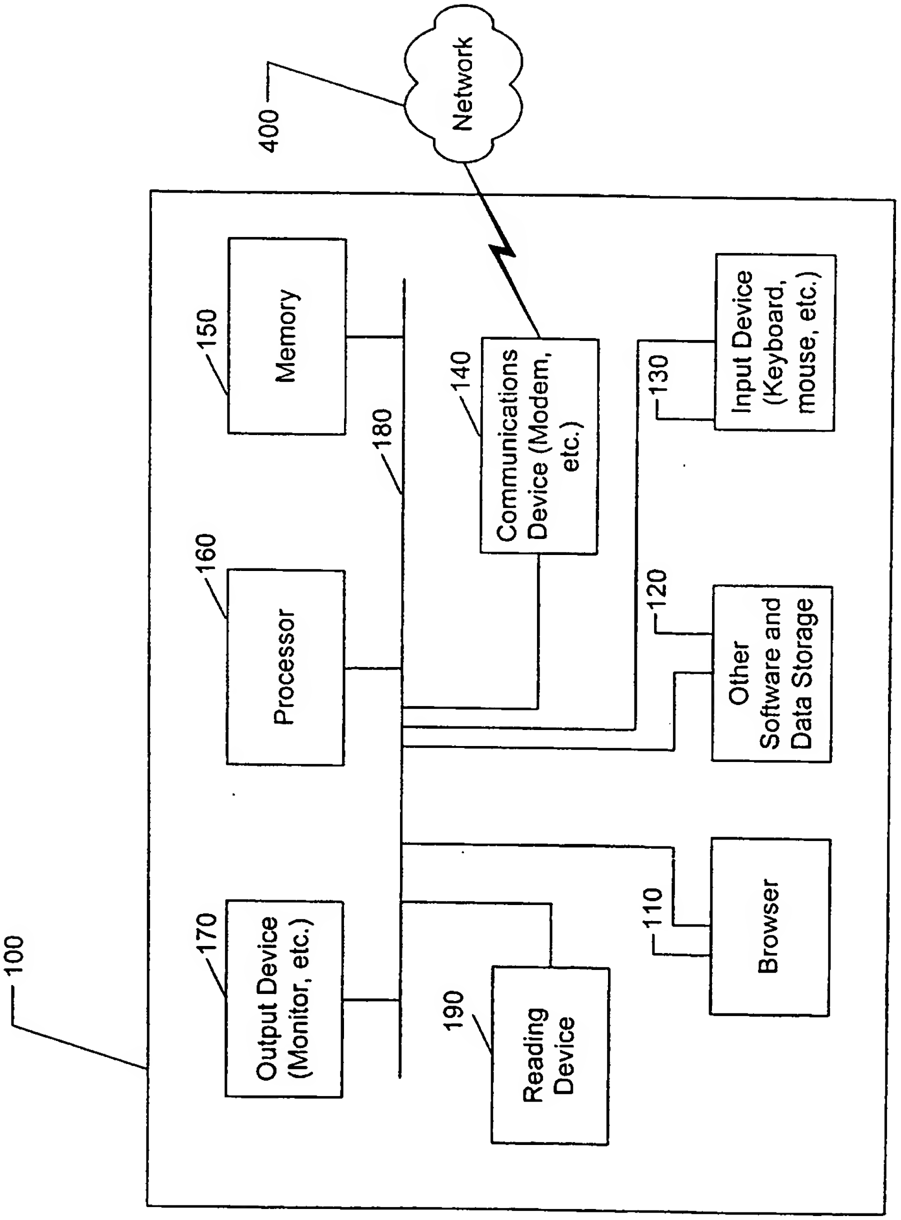

100
Output Device (Monitor, etc.)
170
Processor
160
Memory
150
180
Network
400
Communications Device (Modem, etc.)
140
Reading Device
190
Browser
110
Other Software and Data Storage
120
Input Device (Keyboard, mouse, etc.)
130

FIG. 2

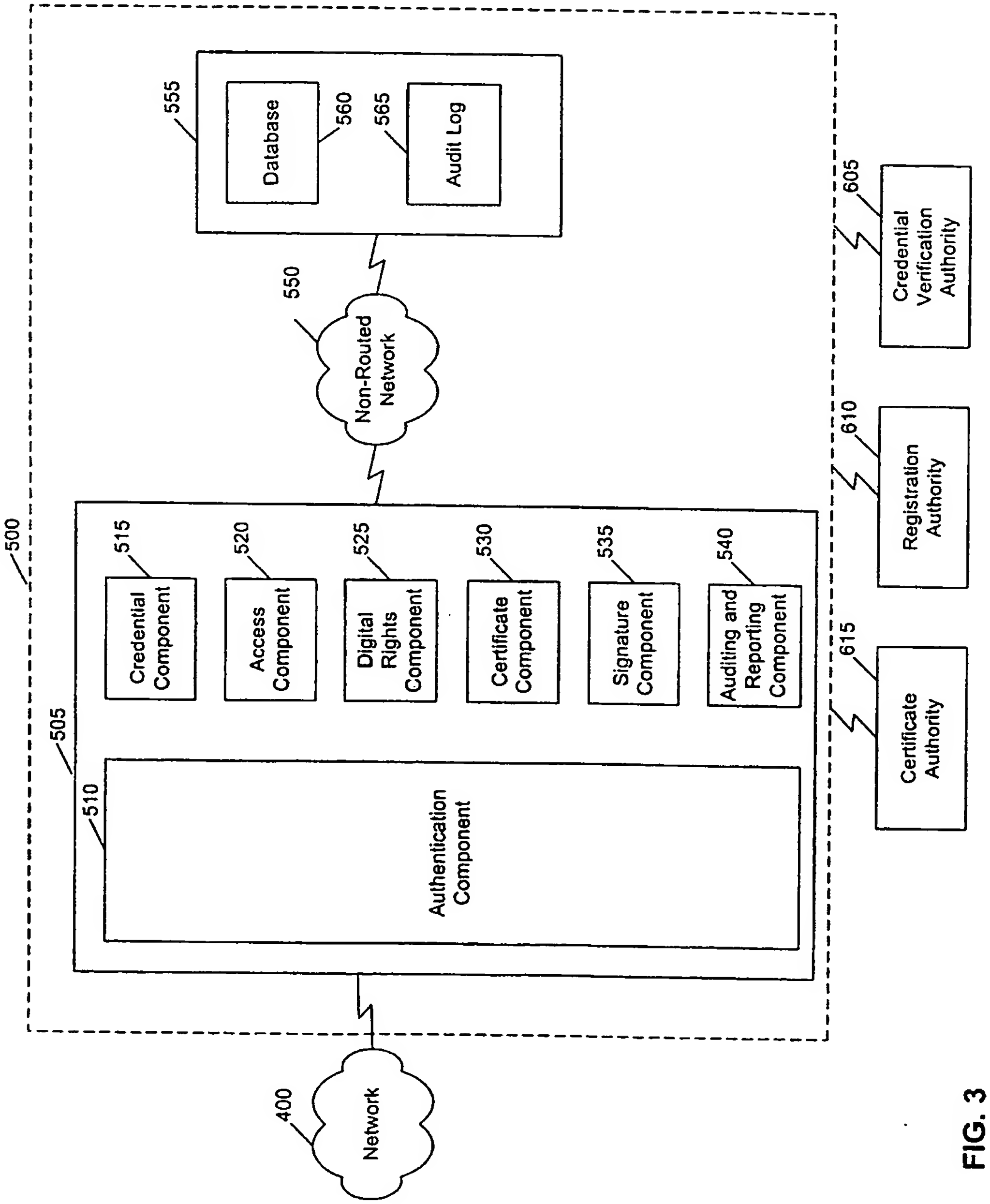

500
505
510
Authentication Component
515
Credential Component
520
Access Component
525
Digital Rights Component
530
Certificate Component
535
Signature Component
540
Auditing and Reporting Component
550
Non-Routed Network
555
560
Database
565
Audit Log
400
Network
605
Credential Verification Authority
610
Registration Authority
615
Certificate Authority

FIG. 3

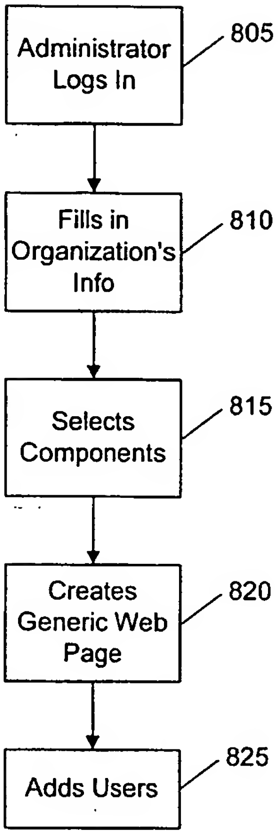

Administrator Logs In
805
Fills in Organization's Info
810
Selects Components
815
Creates Generic Web Page
820
Adds Users
825

FIG. 4

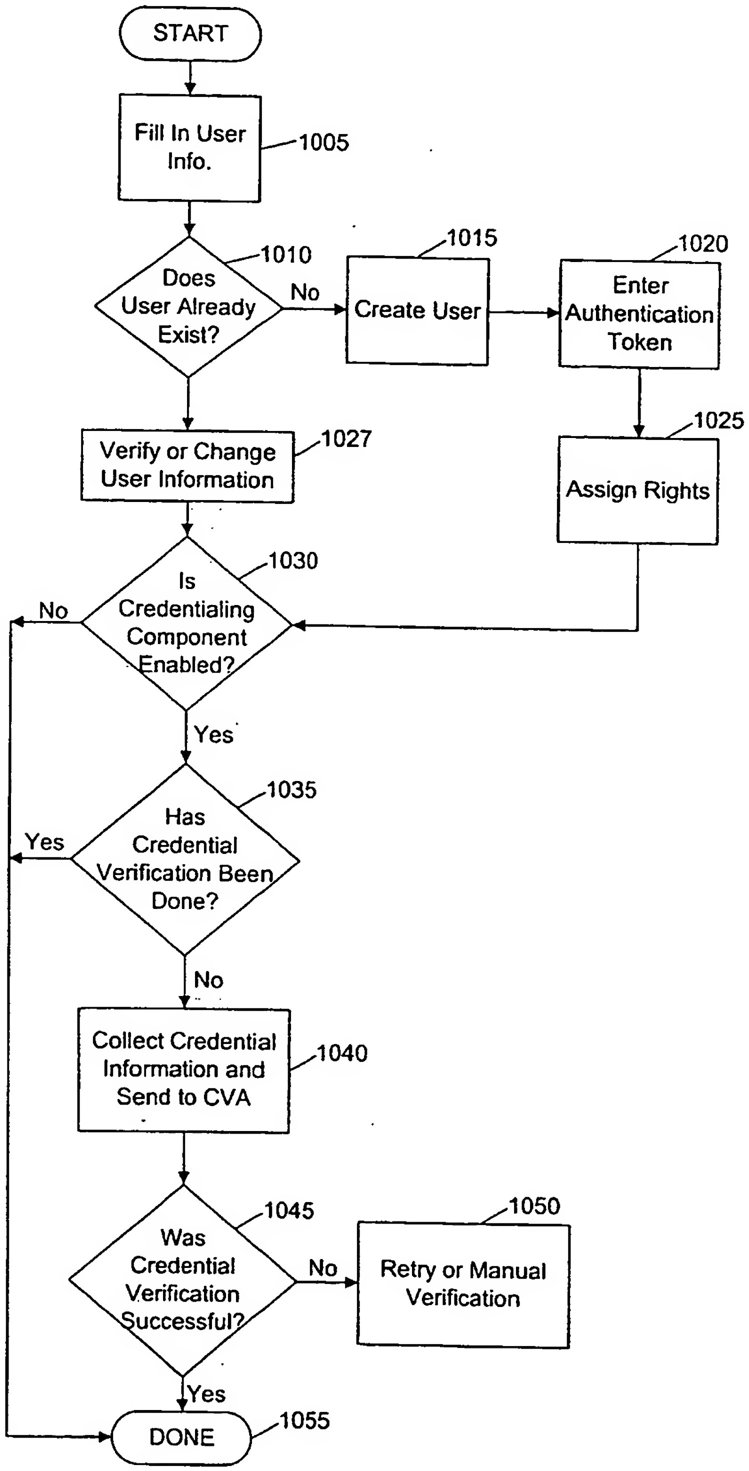

START
Fill In User Info.
1005
Does User Already Exist?
1010
No
Create User
1015
Enter Authentication Token
1020
Assign Rights
1025
Verify or Change User Information
1027
Is Credentialing Component Enabled?
1030
No
Yes
Has Credential Verification Been Done?
1035
Yes
No
Collect Credential Information and Send to CVA
1040
Was Credential Verification Successful?
1045
No
Retry or Manual Verification
1050
Yes
DONE
1055

FIG. 5

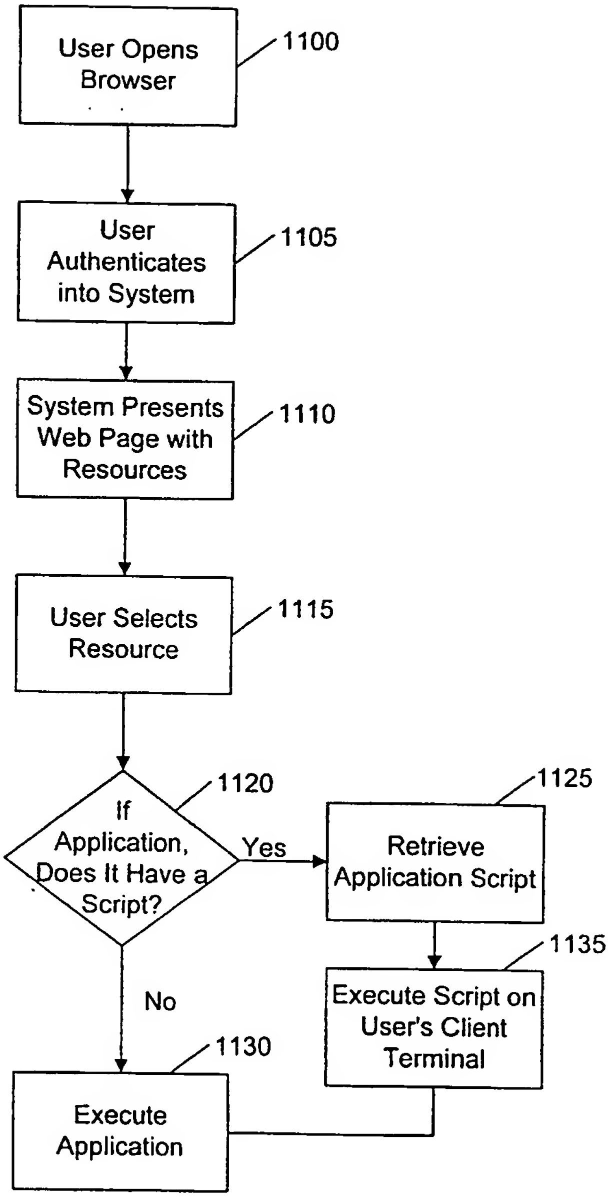

User Opens Browser
1100
User Authenticates into System
1105
System Presents Web Page with Resources
1110
User Selects Resource
1115
If Application, Does It Have a Script?
1120
Yes
Retrieve Application Script
1125
Execute Script on User's Client Terminal
1135
No
1130
Execute Application

FIG. 6

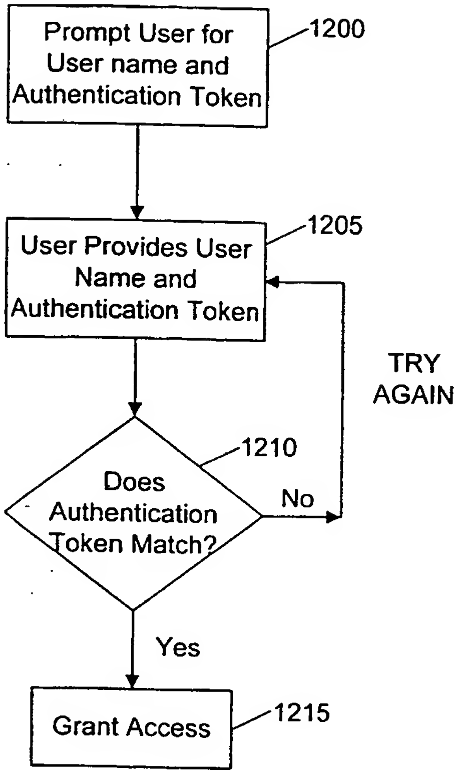

Prompt User for User name and Authentication Token
1200
User Provides User Name and Authentication Token
1205
TRY AGAIN
Does Authentication Token Match?
1210
No
Yes
Grant Access
1215

FIG. 7

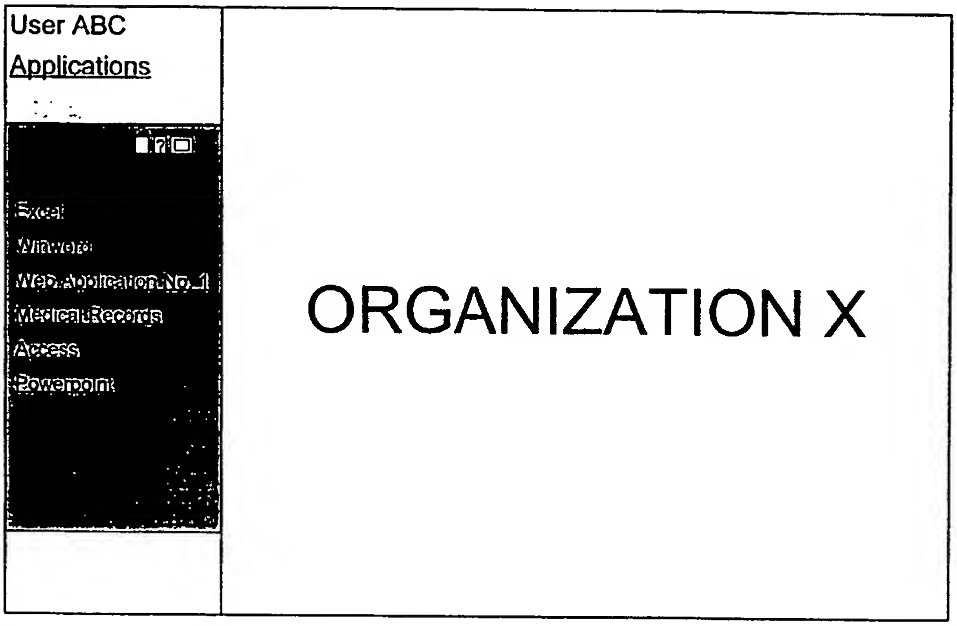

User ABC
Applications
Excel
Winword
Web Application No. 1
Medical Records
Access
Powerpoint
ORGANIZATION X

FIG. 8

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PCT/US 00/17681

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 875 296 A (AULT MICHAEL BRADFORD ET AL) 23 February 1999 (1999-02-23) abstract; figures 1,3,4 column 1, line 9 - line 38 column 2, line 26 -column 3, line 46 column 8, line 14 -column 9, line 20	1,2,4,9,10,12,17,18,20
Y		5-8,13-16,21-24

X	WO 98 57247 A (KONINKL PHILIPS ELECTRONICS NV ;PHILIPS AB (SE)) 17 December 1998 (1998-12-17) abstract; figure 1 page 1, line 1 - last line page 5, line 13 - line 27 page 15, line 29 -page 16, line 24	1,3,9-11,17-19

	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 28 September 2000	Date of mailing of the international search report 06/10/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Powell, D

Interr nal Application No
PCT/US 00/17681

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 42041 A (OPEN MARKET INC) 27 December 1996 (1996-12-27) abstract; figures 1,2B,3,5 page 5, line 8 -page 14, line 29 page 15, line 9 -page 17, line 2	1,9,17
Y		8,16,24

Y	N ISLAM ET AL: "A Flexible Security Model for Using Internet Content" IBM, THOMAS J. WATSON RESEARCH CENTER, 'Online! 28 June 1997 (1997-06-28), XP002138803 Retrieved from the Internet: <URL:http://www.ibm.com/java/education/flexsecurity/> 'retrieved on 2000-05-25! the whole document	5-7, 13-15, 21-23

A	US 5 892 904 A (ATKINSON ROBERT G ET AL) 6 April 1999 (1999-04-06) abstract; figures 2A,3,4 claims 1-31	5,7,13, 15,17-24

1

INTERNATIONAL SEARCH REPORT

.ormation on patent family members

Interr nal Application No
PCT/US 00/17681

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
US 5875296	A	23-02-1999	JP	3003997	B	31-01-2000
			JP	10257048	A	25-09-1998
WO 9857247	A	17-12-1998	US	5930804	A	27-07-1999
			EP	0923756	A	23-06-1999
WO 9642041	A	27-12-1996	US	5708780	A	13-01-1998
			US	5812776	A	22-09-1998
			AU	694367	B	16-07-1998
			AU	5936796	A	09-01-1997
			CA	2221506	A	27-12-1996
			EP	0830774	A	25-03-1998
			JP	11507752	T	06-07-1999
US 5892904	A	06-04-1999	NONE			